1. DEFINIÇÃO

Esta Instrução Normativa, devidamente aprovada pelo Conselho de Administração, estabelece os critérios a serem adotados pelos colaboradores, diretores e conselheiros da Cooperativa de Economia e Crédito Mútuo dos Empregados da CBMM Ltda, denominado Cooperativa, à resolução 4.893 de 26 de fevereiro de 2021, do Banco Central do Brasil, que estabelece a implementação da Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados de computação em nuvem.

2. OBJETIVO

São objetivos da Política de Segurança Cibernética:

I – Assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) da Cooperativa, impedir e dificultar sua utilização contra os interesses da mesma.

II – Capacitar e gerir talentos humanos necessários à conduta ética e segura das atividades no âmbito tecnológico da Cooperativa;

III – Prover uma base comum para as práticas efetivas de gestão de segurança cibernética;

IV - Viabilizar a confiança nos relacionamentos entre a Cooperativa e seus colaboradores.

3. CAMPO DE APLICAÇÃO

As tarefas descritas nesta IN são aplicáveis a todos os colaboradores da Cooperativa, inclusive diretores e conselheiros, indistintamente, devendo ser observados os procedimentos para sua execução, e a mesma deverá ser revisada no mínimo anualmente.

4. RESPONSABILIDADES E AUTORIDADES

4.1 **Colaboradores Cooperativa:** É de obrigação de todas as áreas e colaboradores, executarem, observarem e cumprirem as normas que constam nesta IN.

4.2 **Diretoria Executiva:** Analisar e efetuar em conjunto com a Gerência da Cooperativa, a implementação e aquisição de novos sistemas, bem como acompanhar a área de TI na administração e controle da segurança de sistemas, computadores e rede. O Diretor Coordenador será responsável pela Política de

Segurança Cibernética e pela execução do plano de ação e de resposta a incidentes.

Comunicar tempestivamente ao Banco Central do Brasil as ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise, bem como as providências tomadas para o reinício das atividades.

4.3 **Conselho Administrativo:** É responsabilidade do Conselho de Administração aprovar, supervisionar e revisar, sempre que necessário, a presente política, garantindo a gestão de toda segurança cibernética da Cooperativa.

4.4 **Conselho Fiscal:** Acompanhar a execução desta IN.

4.5 **Gerência e Agente de Controle Interno:**

- Definir as permissões de acesso ao sistema, restringindo e controlando o acesso dos usuários;

- Administrar o acesso de usuários aos sistemas e máquinas de acordo com suas necessidades;

- Elaborar o relatório anual referente a implementação do plano de ação e de resposta a incidentes;

- Monitorar, em conjunto com a empresa responsável a infraestrutura de rede, realizando, periodicamente testes e varreduras no sistema que permitam identificar vulnerabilidades dos softwares de detecção de vírus e problemas/falhas no firewall da rede;

- Acompanhar, periodicamente, os relatórios de auditoria do sistema monitorando as ações realizadas, notadamente, aquelas vinculadas a criação e alteração de dados;

- Divulgar as linhas gerais da política de segurança cibernética, aos colaboradores, conselheiros, fornecedores e cooperados, atentando para uma linguagem clara e acessível a todos os públicos;

- Implementar programas de treinamento, cientificando e capacitando os colaboradores quanto a importância de manter a segurança da informação.

5. RAZÕES, AMEAÇAS E RISCOS CIBERNÉTICOS

Os avanços tecnológicos criam facilidades que possibilitam o uso de novas ferramentas para a atuação das Instituições Financeiras, permitindo assim agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços.

Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições.

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas, hackers individuais, terroristas, colaboradores, competidores, etc) como por exemplo:

- Ganhos financeiros através de roubo, manipulação ou adulteração de informações;

- Obter vantagens competitivas e informações confidenciais de Clientes ou Instituições concorrentes;

- Fraudar, sabotar ou expor a Instituição invadida por motivos de vingança, ideias políticas ou sociais;

- Praticar o terror e disseminar pânico e caos;

- Enfrentar desafios e/ou ter adoração por hackers famosos.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade e informações/bens de cada organização. As consequências para as Instituições podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial, alem disso riscos operacionais. Os possíveis impactos dependem também da rápida detecção e resposta após a identificação do ataque.

Tanto instituições maiores como menores podem ser impactadas e por esse motivo os ativos incorporados no espaço cibernético devem ser protegidos e preservados, sendo também essa necessidade um dos motivos da implementação desta Política.

Entre esses ativos cibernéticos estão:

- Softwares, como um programa de computador;

- Conectividades como acesso à Internet, Banco Central, Receita Federal, etc;

- Informações sigilosas de cooperados;

• Componentes físicos, como servidores, estações de trabalho, notebooks, etc.

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, reguladores de mercado, incluindo o Banco Central através da Resolução 4.893/21 já mencionada, têm voltado maior atenção para esse assunto com o objetivo de orientar as instituições em seus respectivos mercados e verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

Princípios:

A segurança da informação é baseada em três pilares:

I – Confidencialidade: busca garantir de que a informação é acessível somente por pessoas autorizadas;

II – Integridade: Salvaguarda da exatidão e completude da informação;

III – Disponibilidade: garantia de acesso à informação sempre que preciso.

6. NORMAS GERAIS

A Segurança da informação da Cooperativa estabelece os principais controles, denominados diretrizes:

a) As informações da Cooperativa, dos cooperados e de todos envolvidos devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

b) A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

c) Todo processo, durante o seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador, para que a atividade não seja executada e controlada por uma única pessoa.

d) O acesso às informações e recurso só deve ser feito se devidamente autorizado.

e) A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

f) A concessão de acessos deve obedecer critérios de menor privilégio, no qual os usuários têm acesso somente aos recursos e informações imprescindíveis para o pleno desempenho de suas atividades.

g) A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

h) Os riscos às informações da Cooperativa devem ser reportados ao Diretor que é responsável pela Política de Segurança Cibernética.

i) As responsabilidades quanto à segurança da Informação devem ser amplamente divulgadas aos colaboradores, que devem entender e assegurar estas diretrizes.

Conforme a Resolução n° 4.893/21, os serviços de computação em nuvem abrangem a disponibilidade da Cooperativa, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

a) Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a Cooperativa implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos internos adquiridos.

b) Implantação ou execução de aplicativos desenvolvidos ou adquiridos pela Cooperativa utilizando recursos computacionais de seus prestadores de serviços.

c) Execução por meio de Internet de aplicativos implantados ou desenvolvidos por prestadores de serviços da Cooperativa, com utilização de recursos computacionais do próprio prestador de serviços contratado pela Cooperativa.

A Cooperativa é responsável pela Gestão dos serviços contratados incluindo as seguintes atividades:

a) Análise de informações e de recursos adequados ao monitoramento dos serviços;

b) Confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados junto a Prestadores de serviços;

c) Cumprimento da legislação e da regulamentação vigente.

Implementação:

A implementação desta Política considera as seguintes compatibilidades da Cooperativa:

a) O porte, perfil de risco e o modelo de nossos negócios;

b) A natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais.

c) A sensibilidade dos dados e das informações sob responsabilidade da instituição.

Os ambientes, sistemas, computadores e redes da Cooperativa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Caberá todos os colaboradores conhecer e adotar as disposições desta política e deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não autorizadas, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas ao exercícios de suas atividades.

7. PROCEDIMENTOS E CONTROLES

No intuito de registrar procedimentos e controles para reduzir a vulnerabilidade da Cooperativa a incidentes e atender aos demais objetivos de segurança cibernética, e através disso prover controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis, apresentamos a seguir as principais orientações para manter o computador seguro:

I – Manter os softwares de detecção e proteção (anti vírus), atualizados, capazes de proteger eficientemente o ambiente corporativo.

II – Manter atualizados os softwares e aplicativos de uso na rede.

III – Somente instalar programas legítimos, de fonte confiáveis.

IV – Não abrir e-mails e arquivos enviados de fontes desconhecidas.

V – Ao compartilhar recursos dos computadores, estabelecer senhas para os compartilhamentos e permissões de acesso adequadas.

VI – Ficar atento aos endereços acessados nos navegadores.

VII– Na utilização de internet banking procurar pelos sinais de segurança.

VIII – Trocar as senhas com frequência, ela é pessoal e intransferível, e, criada de acordo com as funções permitidas para o exercício das suas atividades.

IX – A maioria das redes sem fio usa algum tipo de configurações de segurança. Essas configurações de segurança definem a autenticação (como o dispositivo se identifica para a rede) e a criptografia (como os dados são criptografados à medida que são enviados através da rede). Procurar sempre acessar redes seguras.

X – Ao detectar algum erro é importante que seja rastreado, através das tecnologias disponíveis todo o caminho do processo, para, assim, corrigir o ponto onde o erro aconteceu ou iniciou.

XI – Realizar backup periodicamente de todos os arquivos e sistema

Ressaltamos que a simples aplicação destas recomendações, auxilia, porém não garante a segurança da informação. Orientamos que no caso de dúvida não seja executado nenhum procedimento sem conhecimento e orientação específica de pessoas regularmente habilitadas para sanar quaisquer dúvidas e executar procedimentos de segurança.

Os procedimentos acima descritos buscam abranger no mínimo a autenticação, criptografia, prevenção, detecção e possíveis vazamentos de informação, a realização periódica de testes e varreduras para detecção de vulnerabilidade, bem como a proteção contra software maliciosos, e o estabelecimento de mecanismos de rastreabilidade. Busca prover ainda, o controle de acesso e segmentação da rede, a manutenção de cópias de segurança dos dados e das informações e o desenvolvimento de sistemas seguros.

Além das informações citadas acima, o Conselho de Administração aprovou a elaboração do plano de ação para implementação da Segurança Cibernética e Planilha de Controle de Riscos.

8. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Cooperativa adota os seguintes processos:

8.1 Gestão de Ativos da Informação:

Entende-se por Ativos da Informação todos os tipos de dados que se pode criar, processar, armazenar, transmitir, alterar e excluir. Podem ser tecnológicos (“software” e “hardware”) e não tecnológicos (pessoas, processos e dependências físicas).

Os ativos da informação devem ser identificados de forma individual, inventariado e protegido de acesso indevido, fisicamente e logicamente, ter documentos e planos de manutenção.

8.2 Classificação da Informação:

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Confidencial, Restrita, Interna, Pública e Sensível. Para isso, devem ser consideradas as necessidades

relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Confidencial: É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da Cooperativa. São protegidas, por exemplo, por criptografia. Dados confidenciais devem ser usados quando existe uma pessoa especifica que pode recepcioná-los.

Restrita: É o nível médio de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores. Podem ser protegidas, por exemplo, restringindo o acesso à uma pasta ou diretório da rede.

Interna: Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da Cooperativa, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

Pública: São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público. No entanto, sempre cabe lembrar dos outros dois pilares: a disponibilidade e a integridade.

Sensível: Para as questões que envolvem a LGPD.

8.3 Gestão de Acessos:

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da Cooperativa.

Os acessos devem ser rastreáveis, a fim de garantir que ações sejam passíveis de auditoria e possam identificar individualmente o colaborador, para que seja responsabilizado por suas ações.

8.4 Gestão de Riscos:

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidade, ameaças e impactos sobre os ativos de informação da Cooperativa, para que sejam recomendadas as proteções adequadas.

Os cenários de riscos de segurança da informação são escalonados nos setores apropriados, para decisão.

8.5 Tratamento de Incidentes:

Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam os negócios da Cooperativa, como por exemplo:

- Queda de energia elétrica;
- Falha de um elemento de conexão;
- Servidor fora do ar;
- Ausência de conexão com internet;
- Sabotagem/terrorismo;
- Indisponibilidade de acesso a cooperativa;
- Ataques DDOS.

Qualquer colaborador que detectar um incidente deverá comunicar imediatamente ao Diretor Responsável pela Política de Segurança Cibernética.

8.6 Segurança Física do Ambiente:

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas.

8.7 Controle de Prestadores de Serviços que Manuseiam Dados ou Informações Sensíveis

Os prestadores de serviços que detenham informações sensíveis ou que sejam relevantes para condução das atividades operacionais da Cooperativa, deverão ser orientados sobre a Política de Segurança Cibernética e estão cientes que poderão ser responsabilizados sobre qualquer dano ou vazamento de informações de acordo com contrato de prestação de serviço e políticas internas da instituição. O acesso a qualquer informação deverá ser solicitado formalmente por e-mail, a Gerência Administrativa da Cooperativa.

9. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

A Cooperativa promove a disseminação dos princípios e diretrizes de Segurança Cibernética por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da informação.

10. PRESTAÇÃO DE INFORMAÇÕES SOBRE PRECAUÇÃO NA UTILIZAÇÃO DE PRODUTOS E SERVIÇOS FINANCEIROS

A Cooperativa irá fornecer através de suas mídias sociais as principais orientações sobre precauções na utilização de produtos e serviços financeiros.

11. MELHORIA CONTÍNUA DE PROCEDIMENTOS

A Cooperativa deve estar comprometida com a melhoria contínua dos procedimentos relacionados a Segurança Cibernética e sempre que necessário deverá realizar investimentos.

Conforme criticidade, a Cooperativa deverá adotar:

Ações críticas – Consiste de correções emergenciais e imediatas para mitigar riscos iminentes;

Ações de Sustentação – Iniciativas de curto/ médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da Cooperativa e permitindo que ações de longo prazo/ estruturantes possam ser realizadas;

Ações Estruturantes – Iniciativas de médio / longo prazo que tratam a causa raiz dos riscos e que preparam a Cooperativa para o futuro.

Ações de prevenção – Consideramos ações de proteção aquelas que mantêm o bom funcionamento e a efetividade da segurança cibernética da Cooperativa. Exemplo:

- Manter inventários atualizados de hardware e software, bem como verificá-los com frequência para identificar elementos estranhos à instituição. Exemplo: computadores não autorizados ou softwares não licenciados;

- Manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

12. PLANO DE AÇÃO E RESPOSTA A INCIDENTES

Visando a implementação das práticas da Política de Segurança Cibernética, a Cooperativa está implantando um Plano de Ação e de Resposta e Incidentes abrangendo o seguinte:

- Ações a serem desenvolvidas para adequar a estrutura organizacional e operacional aos princípios e diretrizes da Política de Segurança Cibernética;

• Os procedimentos, rotinas, controles e tecnologias a serem utilizadas na prevenção e na resposta a incidentes;

• Área responsável pelo registro e controle dos feitos de incidentes relevantes.

O plano de ação e de Resposta a Incidentes será aprovado pelo Conselho de Administração, registrado em ata do respectivo conselho, e revisado anualmente, caso sejam identificadas oportunidades de melhoria.

12.1 Relatório sobre Implementação do Plano de Ação e de Resposta a Incidentes:

O Agente de Controles Internos da Cooperativa será o responsável pelos registros e controles de incidentes bem como a resposta dada a estes incidentes. Deverá também, preencher o Relatório Anual de Plano de Ação e Resposta a Incidentes, com data base de 31 de dezembro. Anexo I desta IN.

O relatório deverá abordar no mínimo:

• A efetividade da implementação das ações relativas à implementação da Política de Segurança Cibernética;

• O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e tecnologias a serem utilizados na prevenção e na resposta a incidentes;

• Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

• Os resultados de testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

13. GERENCIAMENTO DE INCIDENTES

Tem o objetivo de assegurar que os eventos de segurança de informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre os sistemas de informação da Cooperativa.

O procedimento padronizado para o tratamento de incidentes de segurança compreende as seguintes etapas:

I – Recepção da denúncia de atividade suspeita: Serão aceitas denúncias e a Cooperativa colaborará plenamente com a polícia e entidades legalmente competentes na investigação de atividades presumidamente ilícitas provenientes da rede da Cooperativa, e serão investigados os alertas provenientes dos

sistemas de monitoramento da rede, iniciando o processo de tratamento de incidentes de segurança quando for observada atividade em desacordo com procedimentos éticos e padrões.

II – Medidas de contenção imediata do incidente: A contenção imediata do incidente se fará por meio de bloqueio de acesso do host envolvido à rede até o termino da investigação.

III – Coleta de informações e evidências: Serão coletadas informações e evidências sobre as atividades denunciadas através dos logs dos diversos sistemas e serviços disponíveis na rede da Cooperativa.

IV – Analise das informações e evidências: Todas as informações e evidências serão analisadas para investigar o host que gerou o incidente denunciado. A identificação do host compreenderá a determinação do seu endereço IP e endereço MAC da interface de rede, nome, switch, porta de acesso, usuário e todas outras informações possíveis.

O tipo de atividade será determinado pelas informações evidenciadas em logs de serviços. As evidências necessárias serão compiladas para a formalização da notificação dos envolvidos.

V – Notificação dos envolvidos: Será encaminhada notificação por escrito da atividade denunciada ou sob investigação à direção da Cooperativa. Cabe ao responsável pelos usuários da maquina alvo de investigação a determinação da origem da atividade, com sua adequada comprovação.

Como origem das atividades pode considerar:

a) Atividade realizada pelo usuário;

b) Atividade realizada por terceiro com autorização do usuário;

c) Atividade realizada por invasor, sem autorização ou conhecimento do usuário.

Como evidência da origem da atividade pode-se considerar:

a) Logs de acesso local ou remoto na máquina;

b) Logs de detecção de vírus, spyware, malware, etc...

c) Outras informações que possam identificar claramente a origem da atividade.

VI – Análise crítica e medidas corretivas: A Diretoria notificada com auxílio do responsável pela tecnologia da CoopCredmais avaliará a resposta e determinará as medidas corretivas no host identificado. Nos casos comprovados de invasão e

de atividades maliciosas por parte do usuário, o host permanecerá bloqueado até a implantação das medidas corretivas apresentadas.

Qualquer reclamação em relação à utilização ilícita ou questões de segurança do sistema ou da rede, uso indevido de correio eletrônico, violação de direitos autorais ou qualquer atividade em desacordo com a política devem ser enviadas para o e-mail oficial da Cocban, com a devida comprovação da atividade.

A Diretoria será responsável pela avaliação da melhor forma de compartilhamento das informações sobre incidentes relevantes ora identificados. Tal decisão deverá ser analisada em reunião do Conselho e descrita em ata do mesmo.

13.1.1 Avaliação Inicial

Avaliar o incidente em conjunto com o Conselho de Administração para verificar se é provável a sua reincidência ou se é um sintoma de problema crônico, para a tomada de providências e medidas corretivas. Analisar motivos e consequências imediatas, bem como a gravidade da situação.

13.1.2 Incidente Caracterizado

Deverão ser tomadas as medidas imediatas, tais como:

- O Diretor responsável pela política de Segurança Cibernética avaliará o impacto do incidente nos diversos riscos envolvidos;

- Conforme a relevância (sabotagem, terrorismo, etc) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providencias;

- Conforme a relevância do incidente comunicar os cooperados que por ventura tenha sido afetados;

- Comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções de serviços relevantes, que configurem uma situação de crise pela Cooperativa.

13.1.3 Recuperação

Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência de TI acionada e terceiros-chaves notificados.

Quaisquer dados que estejam faltando ou que estejam corrompidos, ou problemas identificados por colaboradores internos devem ser comunicados ao Conselho de Administração.

13.1.4 Retomada

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar a operação normal, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção.

14. EXIGÊNCIAS PARA A CONTRATAÇÃO DE SERVIÇOS

A Cooperativa ao realizar contratações de serviços relevantes e armazenamento de dados e de computação em nuvem, no país ou no exterior deverá adotar procedimentos visando certificar-se de que a empresa contratada atende as seguintes exigências:

a) Adoção de práticas de Governança Corporativa e de Gestão proporcionais a relevância dos serviços que estão sendo contratados e aos riscos que estão expostos, como por exemplo:

I – Se mantém Política de Segurança da Informação;

II – Se possui Plano de Continuidade Operacional;

III – Se as mudanças ou alterações de serviços ou sistemas são registradas e autorizadas quando de sua implantação em produção (Gestão de Mudanças);

IV – Se mantém Gestão de Incidentes.

b) Verificação da capacidade do potencial Prestador de Serviços de forma a assegurar os seguintes requisitos:

I – Cumprimento da legislação e da regulamentação em vigor;

II – Permissão de acesso da Cooperativa aos dados e as informações a serem processadas ou armazenadas pelo Prestador de Serviços;

III – Confidencialidade, Integridade, disponibilidade e recuperação dos dados e das Informações processadas ou armazenadas pelo Prestador de Serviços;

IV – Aderência a certificações que a Cooperativa possa exigir para a prestação do serviço a ser contratado;

V – Acesso da Cooperativa aos relatórios elaborados por empresa de Auditoria especializada independente contratada pelo Prestador de Serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;

VI – Provimento de informações e de recursos de Gestão adequados ao monitoramento dos serviços a serem prestados;

VII – Identificação e segregação dos dados dos clientes da Cooperativa por meio de controles físicos e lógicos;

VIII – Qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados.

14.1 Avaliação dos Serviços a Serem Contratados

A Cooperativa deve proceder a uma avaliação da relevância dos serviços prestados por empresa com possibilidade de serem contratadas considerando o seguinte:

I – Criticidade dos serviços a serem prestados;

II – Sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas pela empresa contratada;

III – Verificação quanto a adoção, por parte do prestador de serviços quanto a adoção de controles que mitiguem efeitos eventuais vulnerabilidade na liberação de novas versões de aplicativos no caso de serem executados através de internet.

15. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

A Cooperativa, tendo em vista a necessidade de agilizar o atendimento de seus cooperados e visando maior segurança e celeridade, fez a contratação do Serviço de Computação em Nuvem.

O contrato foi firmado com a empresa Rezek Ferreira Informática ltda – Fácil Informática e terá todo o sistema faccred – e os dados operacionalizados por ele – hospedados em datacenter com disponibilidade de tempo (99,97%), em nuvem, utilizando a estrutura da empesa Amazon.

A hospedagem em nuvem dispensa a aquisição de licenças dos softwares de banco de dados, sistema operacional e antivírus, necessários aos servidores em nuvem.

A empresa contratada realizará o backup em nuvem, totalmente automatizado, em ambiente de alta disponibilidade e durabilidade, com garantia da integridade dos dados por meio de restaurações periódicas em ambiente de homologação e confidencialidade das informações.

A empresa contratada monitorará o banco de dados, incluindo o dimensionamento, instalação e configuração até tuning, backup/recover, monitoramento e aplicação de patches.

A empresa contratada realizará o monitoramento de servidores e serviços,

notificando em caso de falhas, mantendo características proativas (ações para antecipação de falhas), reativas (ações de respostas a eventuais falhas) e preventivas (ações para minimizar probabilidade de falhas).

A empresa contratada deverá implementar e manter controles de segurança incluindo, sem limitação, segurança de hardware e software, firewalls, filtros e outras ferramentas de segurança.

A empresa contratada se responsabilizará por armazenar e transmitir as credenciais de acesso e demais informações confidenciais de maneira criptografada.

A empresa contratada deverá garantir a segregação de acesso entre os ambientes de seus diferentes clientes, impedindo o acesso não autorizado às informações.

Caberá à empresa contratada disponibilizar informações para auditorias (internas e externas) e investigações judiciais quando solicitadas.

O Backup,deverá ser realizado de acordo com a periodicidade abaixo descrita, mantendo cada um dos backups efetuados sob a política cíclica de armazenamento, que garante a disponibilidade de restauração de backup dos 7 (sete) últimos dias, com as seguintes características:

- Backup diário de todo o Banco de Dados, utilizando ambiente redundante (replicado) e de alta disponibilidade (99,9999999% de durabilidade e de 99,97% de disponibilidade), inclusive nos sábados, domingos e feriados nacionais; e

- Para garantir a sua integridade, os backups serão testados semanalmente.

15.1 Este Serviço em Nuvem Compreende:

- Ferramentas para governança e rastreabilidade de dados;

- Atendimento às exigências legais uma vez que o trabalho da Amazon é realizado em conjunto com órgãos externos de certificação e auditores independentes para fornecer aos clientes informações importantes sobre suas políticas, processos e controles;

- Ferramentas simples e avançadas que permitem a CREDMAIS determinar onde seu conteúdo será armazenado, proteger o conteúdo em trânsito e em repouso e gerenciar o acesso a serviços e recursos da Amazon;

- Políticas e procedimentos formais para estabelecer parâmetros comuns aos funcionários sobre os padrões e diretrizes de segurança da informação. A

política do sistema de gerenciamento de segurança da informação da Amazon estabelece diretrizes para proteger a confidencialidade, integridade e disponibilidade dos sistemas e conteúdo dos clientes;

- Opção de analisar e fazer download de relatórios e detalhes sobre os controles de segurança usando o portal automatizado de relatórios de conformidade disponível na Console de Gerenciamento da Amazon;

- Ferramentas para monitorar anormalidades e verificar notificações de segurança;

- Identificação e separação lógica dos dados do Cliente em nuvem;

- Curso on-line gratuito desenvolvido para apresentar os fundamentos da computação e segurança em nuvem.

- Existência de acordos para a troca de informações entre o Banco Central do Brasil e as autoridades dos países onde os serviços da Amazon podem ser prestados, não causando danos à operação regular da Cooperativa, nem constrangimento à performance do Banco Central do Brasil.

16. COMUNICAÇÃO AO BANCO CENTRAL

A Cooperativa deverá informar previamente ao Banco Central a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

Essa comunicação deve ser realizada 60 dias antes da contratação dos serviços e deve conter as seguintes informações:

a) denominação da empresa a ser contratada;

b) os serviços relevantes a serem contratados;

c) a indicação dos países e das regiões em cada pais onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, nos casos de contratação no exterior.

As alterações contratuais que impliquem modificações nas informações contratuais devem ser comunicadas ao Banco Central no mínimo 60 dias antes da alteração contratual.

A contratação a ser realizada pela Cooperativa de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, deve observar os seguintes requisitos:

a) A existência de convênio para troca de informações entre o Banco Central do

Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

b) Assegurar que a prestação dos serviços não cause prejuízo ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

c) definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e

d) prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio citado nos itens anteriores a cooperativa deverá solicitar autorização do Banco Central para a contratação, observando o prazo e as informações já mencionadas.

A Cooperativa deve assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes e do Banco Central do Brasil e às informações.

16.1 Dos Contratos

Os contratos firmados entre a Cooperativa e as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

a) a indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

b) a adoção de medidas de segurança para a transmissão e armazenamento dos dados;

c) a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;

d) a obrigatoriedade, em caso de extinção do contrato, de:

I – Transferência dos dados ao novo prestador de serviços ou à Cooperativa.

II – Exclusão dos dados pela empresa contratada substituída após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.

e) O acesso da Cooperativa à:

I – Informações fornecidas pela empresa contratada visando o cumprimento das

itens previstos nos itens a,b e c acima;

II – Informações relativas às Certificações exigida pela Cooperativa e aos relatórios de auditoria especializada contratada pelo prestador de serviços;

III – Informações e recursos de Gestão adequados ao monitoramento dos serviços prestados.

f) a obrigação da empresa contratada notificar a cooperativa sobre a subcontratação de serviços relevantes para a Instituição.

g) a permissão de acesso do Banco Central às seguintes informações:

I – contratos e acordos firmados para a prestação de serviços;

II – documentação e informações referentes aos serviços prestados;

III – os dados armazenados;

IV – as informações sobre processamentos;

V - As cópias de segurança dos dados e das informações;

VI – Códigos de acesso aos dados e as informações.

h) a adoção de medidas pela Cooperativa em decorrência de determinação do Banco Central.

i) a obrigatoriedade da empresa contratada manter a cooperativa permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e regulamentação em vigor.

j) o contrato deve também prever, para o caso de decretação de regime de resolução da cooperativa pelo
Banco Central:

I – a obrigação da empresa contratada para a prestação de serviços conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, a documentação e as informações referentes aos serviços prestados, aos dados armazenados e as informações sobre seus processos, as cópias de segurança dos dados e das informações, bem como aos códigos de acesso que esteja em poder da empresa contratada;

II – A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção da empresa contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observando que:

a) A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime da resolução.

b) A notificação prévia deve ocorrer também na situação em que a interrupção for motivada por inadimplência da cooperativa.

16.2 Documentos Disponíveis ao Banco Central

Os seguintes documentos devem ficar à disposição do Banco Central do Brasil pelo prazo mínimo de 5 (cinco) anos:

- Política de Segurança Cibernética;

- Ata de Reunião do Conselho de Administração implementando / aprovando a Política de Segurança Cibernética e suas revisões;

- Documento relativo ao Plano de Ação e de Resposta a Incidentes relatórios a implementação da Política de Segurança Cibernética;

- Relatório anual de Controles Internos e Gerenciamento de Risco no qual devem contemplar o item sobre a implementação do Plano de Ação e de Resposta a Incidentes;

- Documentação sobre os procedimentos relativos à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem;

- Documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, caso isso ocorra;

- Contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;

- Dados, registros e informações relativas aos mecanismos de acompanhamento e de controles com vistas a assegurar a implementação e a efetividade da Política de Segurança Cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

17. COMUNICADOS

A presente IN 014 – Política de Segurança Cibernética deverá ser divulgada a todos os colaboradores da Cooperativa, Conselheiros, Diretores, bem como a todas as empresas prestadoras de serviços terceirizados.

18. ANEXOS

Anexo I – Relatório Anual Plano de Ação e Resposta a Incidentes (Modelo)

Anexo II – Histórico de Revisões

19. VIGÊNCIA

A presente Instrução Normativa entra em vigor em 25/02/2025.

Jose Vander Firmino Gonçalves
Diretor Financeiro

Clodoveu Luciano Caixeta
Diretor Coordenador

Anexo I

RESOLUÇÃO 4893/2021 - RELATÓRIO ANUAL DE PLANO DE AÇÃO E RESPOSTA A INCIDENTES

DATA BASE DO RELATÓRIO.: ____/_____/_____

	AÇÃO	FREQUÊNCIA	RESPONSÁVEL	STATUS
Controle de acesso	Avaliar junto aos colaboradores da Cooperativa se as senhas (Sistema Fácil, rede, arquivos relevantes e outros sistemas) estão sendo alteradas trimestralmente	TRIMESTRAL	Agente de Controles Internos	
Segurança & Tratamento da Informação	Verificar junto a empresa Fácil Informática se o backup do sistema está sendo efetuado conforme periodicidade definida na IN - 014	TRIMESTRAL	Agente de Controles Internos	
	Verificar junto a área de T.I se estão sendo realizados backups dos arquivos armazenados (Word, Excel, PDF, JPG e Outros)	TRIMESTRAL	Agente de Controles Internos	
	Verificar junto a área de T.I se os softwares de proteção estão sendo atualizados e se estão sendo realizados testes e varreduras que permitam identificar vulnerabilidades	TRIMESTRAL	Agente de Controles Internos	
	Verificar junto a área de T.I se está sendo efetuado controle de tráfego de dados através do firewall (por máquina)	TRIMESTRAL	Agente de Controles Internos	
	Realizar controle de acesso dos prestadores de serviços/terceiros	QUANDO NECESSÁRIO	Gerência	
Melhoria Contínua	Registrar os incidentes ocorridos estabelecendo plano de ação e executar as ações para tratativa	TRIMESTRAL	Agente de Controles Internos	
	Realizar levantamento de necessidade de investimentos, com objetivo de melhorar a segurança e organização dos dados da Cooperativa e de seus clientes	SEMESTRAL	Agente de Controles Internos	

INCIDENTE	DATA	ORIGEM	CRITICIDADE	TIPO IMPACTO	TEMPO MÍNIMO RESPOSTA	AÇÃO	RESPONSÁVEL	STATUS	RESULTADOS OBTIDOS

CONSELHO DE ADMINISTRAÇÃO DIRETOR RESPONSÁVEL AGENTE DE CONTROLE INTERNO

VERSÃO	ITEM	HISTÓRICO DA REVISÃO	DATA DA REVISÃO
1.0	Todos	Emissão do documento com aprovação do Conselho de Administração da Cooperativa através da Ata de nr 01/2021.	26/01/2021
2.0	Todos	Emissão do documento com revisão geral e adequação para atendimento ao apontamento 114.1 do RAC exercício ano de 2022, com aprovação do Conselho de Administração da Cooperativa através da Ata de nr 04/2023.	19/04/2023
3.0	Todos	Emissão do documento com revisão geral e adequação para atendimento a Resolução CMN 4893/2021, com aprovação do Conselho de Administração da Cooperativa através da Ata de nr 02/2025.	25/02/2025